

Randall E. Kay (State Bar No. 149369)  
rekay@jonesday.com  
Douglas L. Clark (State Bar No. 279408)  
dlclark@jonesday.com  
JONES DAY  
4655 Executive Drive, Suite 1500  
San Diego, CA 92121.3134  
Telephone: +1.858.314.1200  
Facsimile: +1.844.345.3178

Patrick T. Michael (State Bar No. 169745)  
pmichael@jonesday.com  
Marcus S. Quintanilla (State Bar No. 205994)  
mquintanilla@jonesday.com  
JONES DAY  
555 California Street, Suite 2600  
San Francisco, CA 94104.1501  
Telephone: +1.415.626.3939  
Facsimile: +1.415.875.5700

Attorneys for Plaintiff  
MICRON TECHNOLOGY, INC.

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

MICRON TECHNOLOGY, INC.,  
  
Plaintiff,  
  
v.  
  
UNITED MICROELECTRONICS  
CORPORATION, FUJIAN JINHUA  
INTEGRATED CIRCUIT CO., LTD., and  
DOES 1-10,  
  
Defendants.

**Case No. 4:17-CV-06932-MMC**

**DECLARATION OF MICHAEL  
BANDEMER IN SUPPORT OF MICRON  
TECHNOLOGY, INC.'S  
SUPPLEMENTAL OPPOSITION TO  
UNITED MICROELECTRONICS  
CORPORATION'S MOTION TO  
DISMISS FOR LACK OF PERSONAL  
JURISDICTION**

Judge: Hon. Maxine M. Chesney  
Courtroom: 7 – 19th Floor  
Hearing date: September 21, 2018  
Hearing time: 9:00 a.m.

Complaint Filed: December 5, 2017

**REDACTED VERSION OF  
DOCUMENT(S) SOUGHT TO BE SEALED**

1 I, MICHAEL BANDEMER, declare as follows:

2 1. I am over the age of 18 and am a resident of the State of California. The work  
3 described below was performed by me and/or under my supervision and direction. I have  
4 personal knowledge of the facts stated in this declaration, and, if called as a witness, could testify  
5 competently to the facts stated below.

6 **Background and Experience**

7 2. I am a Managing Director with Berkeley Research Group, LLC, ("BRG") and the  
8 national practice leader for the firm's Discovery and Forensic Technology Services group which  
9 provides, among other things, consulting and expert services in the area of computer forensics,  
10 electronic discovery, and other associated technology advisory services to corporations, law  
11 firms, and governments in the United States and abroad.

12 3. I have more than 20 years of experience in investigations, technology, and  
13 forensic matters. I advise both corporate clients and law firms on information technology, digital  
14 forensics, and e-discovery issues. I have served as the lead investigator in hundreds of matters  
15 and performed or supervised the forensic collection and analysis of electronically stored  
16 information (ESI) from corporate networks, databases, personal computers (Mac and PC),  
17 phones, tablets, external storage devices, internet, and other digital storage media. I am regularly  
18 engaged as a business consultant and an expert for litigation matters to examine computer  
19 evidence for the purpose of identifying, recovering, analyzing, explaining, and reporting the  
20 observed activity and the state of the evidence.

21 4. I am a Certified Information Technology Professional and an EnCase Certified  
22 Computer Examiner. Additionally, I am licensed in the State of California as a Certified Public  
23 Accountant and am also a Certified Management Accountant and Certified in Financial  
24 Forensics.

25 5. Among other professional associations, I am a past and current President of the  
26 High Technology Crime Investigation Association's ("HTCIA") San Diego Chapter and a Board  
27 Member of the international organization as well as a member of the Sedona Conference  
28 Working Group. I have testified at trial in both Federal and State court as well as in evidentiary

1 hearings on digital forensics and e-discovery issues and have served as a court-appointed neutral  
2 expert. A true and correct copy of my curriculum vitae, which summarizes my professional and  
3 educational background, is attached hereto as **Exhibit 1**. My professional time for analysis and  
4 testimony is not contingent on any outcome and is currently billed at \$500 per hour.

### 5 **Scope of Engagement and Key Findings**

6 6. BRG was engaged by Jones Day on behalf of Micron Technology, Inc.  
7 (“Micron”) to conduct an investigation and forensic analysis into the downloading of Micron  
8 computer files from United States based servers by former employees of Micron’s Taiwanese  
9 subsidiary, specifically Kenny Wang (“Wang”) and potentially others employed during the 2015  
10 and early 2016 timeframe when several employees left Micron for employment with United  
11 Microelectronics Corporation (“UMC”).

12 7. To perform my analysis, BRG was provided with access to Micron’s ESI and  
13 network resources, and consulted with knowledgeable Micron personnel, including individuals in  
14 Micron’s IT department. Through those efforts, BRG identified and collected a forensically  
15 preserved image of the laptop computer which I understand was issued to and used by Mr. Wang  
16 during his employment at Micron (“Wang Laptop”) as well as other evidence from Micron  
17 servers based in the United States and abroad.

18 8. Upon examining the forensic image of Wang’s laptop, I sought to determine if  
19 there was suspicious file activity, indicated either by the nature of the particular files accessed or  
20 the times and dates that they were accessed. I also investigated computer usage on the Wang  
21 Laptop prior to Mr. Wang’s departure from Micron, including the use of external storage media  
22 and accessing and downloading of files on the Wang Laptop before Mr. Wang’s departure. My  
23 investigation and forensic analysis of the evidence described below is consistent with steps taken  
24 to obfuscate file activities by installing data-deletion software and erasing files and activity logs.  
25 Notwithstanding those efforts, the Wang Laptop evidences a significant number of files  
26 downloaded from Micron SharePoint servers and repeated access to Micron’s proprietary  
27 Research and Development CAD system, which largely contains pictorial design files of  
28

1 Micron's semiconductor products. I am informed that both the SharePoint and CAD systems are  
 2 housed exclusively on Micron's United States based servers.

### 3 **Evidence Analyzed**

4 9. With the assistance of Micron personnel, BRG identified, preserved, and collected  
 5 the following evidence, which I ultimately relied upon for my analysis:

6 10. **EnCase forensic disk image of Wang's Micron-issued laptop.** Mr. Wang's  
 7 laptop was retained by Micron and, using computer forensic software known as EnCase, a  
 8 forensic image was created on September 16, 2016. A copy of this image was provided to BRG  
 9 for analysis. This image represents a complete bit-by-bit image of the Micron laptop computer  
 10 assigned to Wang prior to his departure from the company. The image was used to collect  
 11 forensic artifacts revealing Wang's computer actions related to file activity, server access, file  
 12 deletion, and software execution. This forensic image included what is known as a "volume  
 13 shadow copy" that was generated on April 24, 2016 ("Shadow Copy") – two days prior to Mr.  
 14 Wang's departure from Micron. A Shadow Copy is essentially a back-up of the computer that  
 15 allows one to reconstruct the contents of the computer back to the time of the Shadow Copy. It  
 16 is created automatically and typically without the user's knowledge.

17 11. We are informed that Mr. Wang had a Google Drive account associated with the  
 18 email address [REDACTED]@gmail.com (the "Wang Google Drive Account"). Internet browsing  
 19 evidence from the Wang Laptop revealed the partial contents of the Wang Google Drive  
 20 Account. Google Drive is a file storage service offered by Google where users can upload, store,  
 21 and share files from local computers and servers on the internet. These files are accessible from  
 22 any computer with access to the internet provided the user knows the associated password and  
 23 user name. There is no log or system that specifically records uploads to the Google servers  
 24 other than Google itself. The forensic artifacts identified on the Wang Laptop relating to Wang's  
 25 use of the Google drive represent only a partial view of the contents of the Wang Google Drive  
 26 Account. Forensic evidence revealed that in April 2016, the Wang Google Drive Account stored  
 27 over 21 gigabytes of data. To put this in perspective, depending on the types of files stored, a  
 28 single gigabyte may represent over 3,000 files. There are file types like Computer Aided Design

1 (“CAD”) drawings and schematics of concern in this matter that take substantially more storage  
 2 than a typical Microsoft Office file.

3 12. **Micron [REDACTED] logs for user Kenny Wang.** It is my  
 4 understanding that in mid-2015, [REDACTED]

5 [REDACTED]  
 6 [REDACTED]  
 7 [REDACTED]  
 8 [REDACTED]  
 9 [REDACTED]  
 10 [REDACTED] These logs [REDACTED] were used in my investigation to identify  
 11 external devices used on the Wang Laptop and the date, time, and name of files transferred.

12 13. **File listings from United States based Microsoft SharePoint servers and**  
 13 **foreign file share servers accessed from the Wang Laptop.** During the forensic analysis of  
 14 the Wang Laptop, evidence of the file server and directory locations frequented by the Wang  
 15 Laptop in 2016 were identified and subsequently, with the help of Micron IT employees, BRG  
 16 obtained file listings of those servers and directories, including:

17 [REDACTED]  
 18 [REDACTED]  
 19 [REDACTED]  
 20 [REDACTED]  
 21 [REDACTED]  
 22 [REDACTED]  
 23 [REDACTED]  
 24 [REDACTED]  
 25 [REDACTED]  
 26 [REDACTED]  
 27 [REDACTED]

14. The file listings from these server and directory locations were ultimately compared to the forensic artifacts on the Wang Laptop and the [REDACTED] logs obtained from the Micron servers to determine whether the files downloaded/copied to the Wang Laptop were obtained from United States based servers and/or elsewhere.

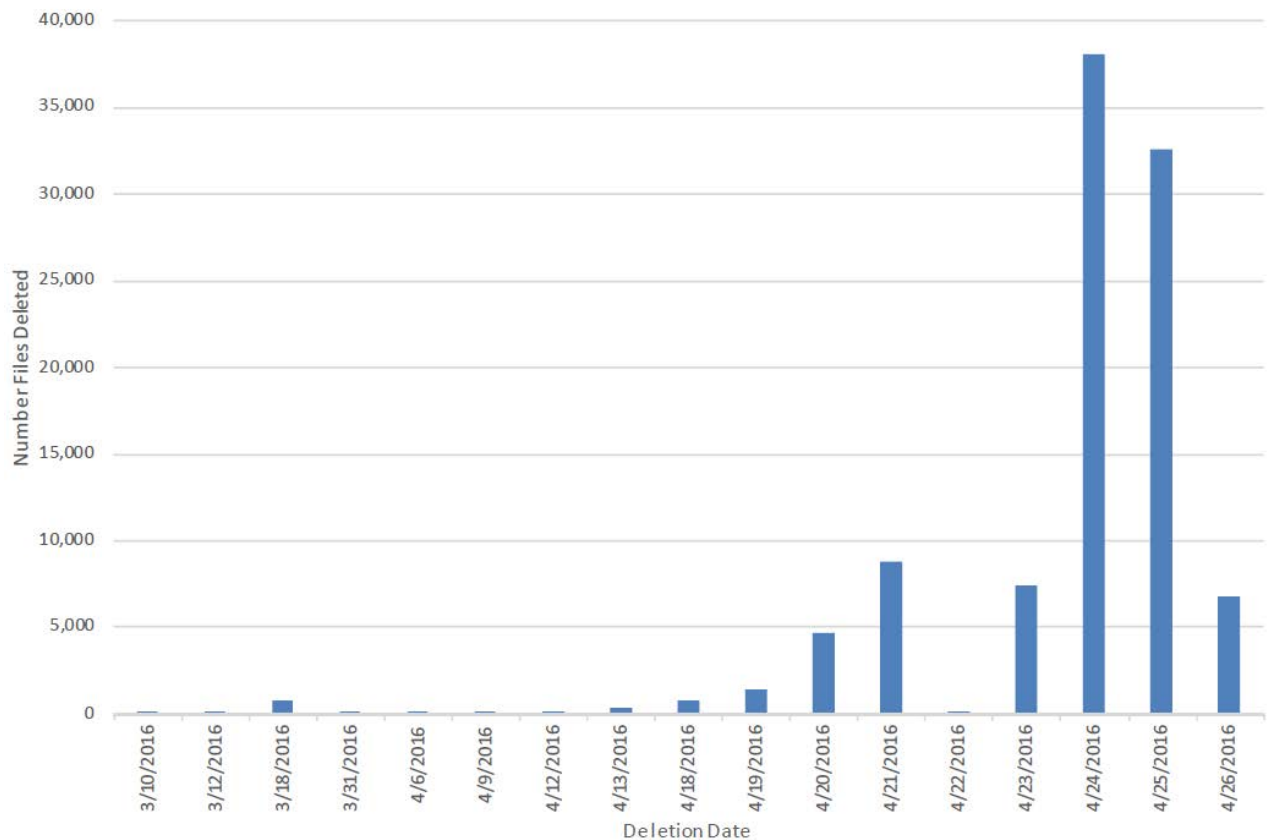
## Detailed Findings

15. My investigation and forensic analysis of the evidence described above indicate that actions on the Wang Laptop prior to and in or around April 26, 2016 (the date of Mr. Wang's departure from Micron) are consistent with the following:

### **Destruction of Evidence:**

16. Shortly before Wang left Micron, a portable version of “system optimizer” software called “CCleaner portable” was downloaded and utilized on the Wang Laptop. CCleaner is frequently used to delete computer data and files that a forensic examiner typically analyzes to ascertain evidence of access, download, and transfer of files from servers to personal external storage devices or personal cloud storage accounts. By design, however, CCleaner portable leaves a small evidence footprint. Evidence of CCleaner being downloaded and used on the Wang Laptop was captured from areas within the computer’s registry that stores historical executions of software called the “Userassist” and “Shimcache”. As reflected in the forensic chronology set forth in **Exhibit 2** to this declaration, in the days and weeks leading up to Mr. Wang’s departure from Micron, there were Google searches for “CCleaner” and several versions of the CCleaner software were then downloaded, run, and afterwards deleted. A true and correct copy of a forensic chronology created by my team is attached hereto as **Exhibit 2**.

17. From March 10, 2016 through April 26 – the last day of Mr. Wang’s employment at Micron – 101,154 items were deleted. Evidence of this deletion activity was observed within the “NTFS USN journal” of the Wang Laptop, which is essentially a log file for file/folder events on the hard-disk. The deletion of files accelerated as Mr. Wang approached his departure date: 77,260 files and folders were deleted in the last three days of his employment. Chart 1 below illustrates the number and frequency of deletions in March/April 2016 and the acceleration of deletions leading up to Wang’s last day of employment.

**Chart (1) – Deletions March and April 2016**

18. Notwithstanding these apparent efforts to delete evidence of file activity, BRG was able to uncover substantial evidence of the downloading and uploading activity on the Wang Laptop through the analysis of computer forensic artifacts and reconstruction of the file system using the Shadow Copy. Nevertheless, use of the CCleaner deletion software on the Wang Laptop makes it impossible to detect all such activity that may have occurred.

#### **SharePoint Downloads:**

19. SharePoint is an internet browser-based collaboration and document management platform from Microsoft that allows groups of employees to centrally store, secure, and share electronic documents with other authorized users of a group. Micron licenses SharePoint and stores its electronic confidential and proprietary documents on Micron SharePoint servers. I understand that since December 2014, all Micron SharePoint servers have been in the United



1 States. I also understand that Mr. Wang was a SharePoint Site Collection Administrator for his  
2 Process Integration group at Micron.

3 20. In 2016 at least 174 Micron files stored on United States based SharePoint servers  
4 were accessed by and/or downloaded to the Wang Laptop. (See a true and correct copy of a  
5 spreadsheet created by my team containing files accessed on a U.S. SharePoint servers and is  
6 attached hereto as **Exhibit 3.**) Of those files, 129 were accessed/downloaded in the two weeks  
7 prior to Mr. Wang's last day of employment on April 26, 2016. (*Id.*) Of the 174 Micron files  
8 accessed from United States based SharePoint servers, the forensic evidence indicates that at  
9 least 36 were downloaded to the Wang Laptop hard drive. (See a true and correct copy of a  
10 spreadsheet created by my team, which contains those files that were downloaded to the Wang  
11 Laptop from a U.S. SharePoint server and is attached hereto as **Exhibit 4.**)

12 21. **Table 1** below, reflects a sub-set of the United States based downloading activity  
13 detected on the Wang Laptop as illustrated in **Exhibit 4** – specifically, downloads from United  
14 States based servers on April 25, 2016, the day before Mr. Wang left Micron. Though it captures  
15 only a small part of the overall United States based downloading detected on Wang's laptop, it  
16 illustrates a consistent pattern. First, accessing a specific file on a United States based  
17 SharePoint server. Then, within seconds or minutes, downloading the same file to the Wang  
18 Laptop. In some cases, evidence shows the downloaded files were further transferred to a  
19 personal external storage device. Micron's [REDACTED] system did not track uploads to the Google  
20 Drive Account, and there is no system or log that would track all file uploads to Wang's Google  
21 Drive Account other than Google itself.

22 **Table (1) – Examples from Exhibit 4 - 4/25/2016**

23 Ref # from Exhibit 4	24 Activity Date <sup>1</sup>	File Location	Server Location	File Name
25 File 20	4/25/16 13:31	collab.micron.com <sup>2</sup>	Boise USA	[REDACTED]

27 <sup>1</sup> All date and times have been normalized to Universal Time Coordinated (UTC).

28 <sup>2</sup> The IP address for this device is 137.201.15.211.



Ref # from Exhibit 4	Activity Date <sup>1</sup>	File Location	Server Location	File Name
	4/25/16 13:34	Laptop		
File 21	4/25/16 14:11	collab.micron.com	Boise USA	
	4/25/16 14:10	Laptop		
File 22	4/25/16 16:01	collab.micron.com	Boise USA	
	4/25/16 16:05	Laptop		
File 23	4/25/16 16:10	collab.micron.com	Boise USA	
	4/25/16 16:11	Laptop		
File 24	4/25/16 16:12	collab.micron.com	Boise USA	
	4/25/16 16:13	Laptop		
File 25	4/25/16 16:14	collab.micron.com	Boise USA	
	4/25/16 16:16	Laptop		
File 26	4/25/16 16:17	collab.micron.com	Boise USA	
	4/25/16 16:18	Laptop		
File 27	4/25/16 16:19	collab.micron.com	Boise USA	
	4/25/16 16:21	Laptop		
File 28	4/25/16 16:24	collab.micron.com	Boise USA	
	4/25/16 16:27	Laptop		
File 29	4/25/16 16:37	collab.micron.com	Boise USA	
	4/25/16 16:39	Laptop		
File 30	4/25/16 16:54	collab.micron.com	Boise USA	
	4/25/16 16:55	Laptop		
File 31	4/25/16 16:57	collab.micron.com	Boise USA	
	4/25/16 16:59	Laptop		
File 32	4/25/16 17:00	collab.micron.com	Boise USA	

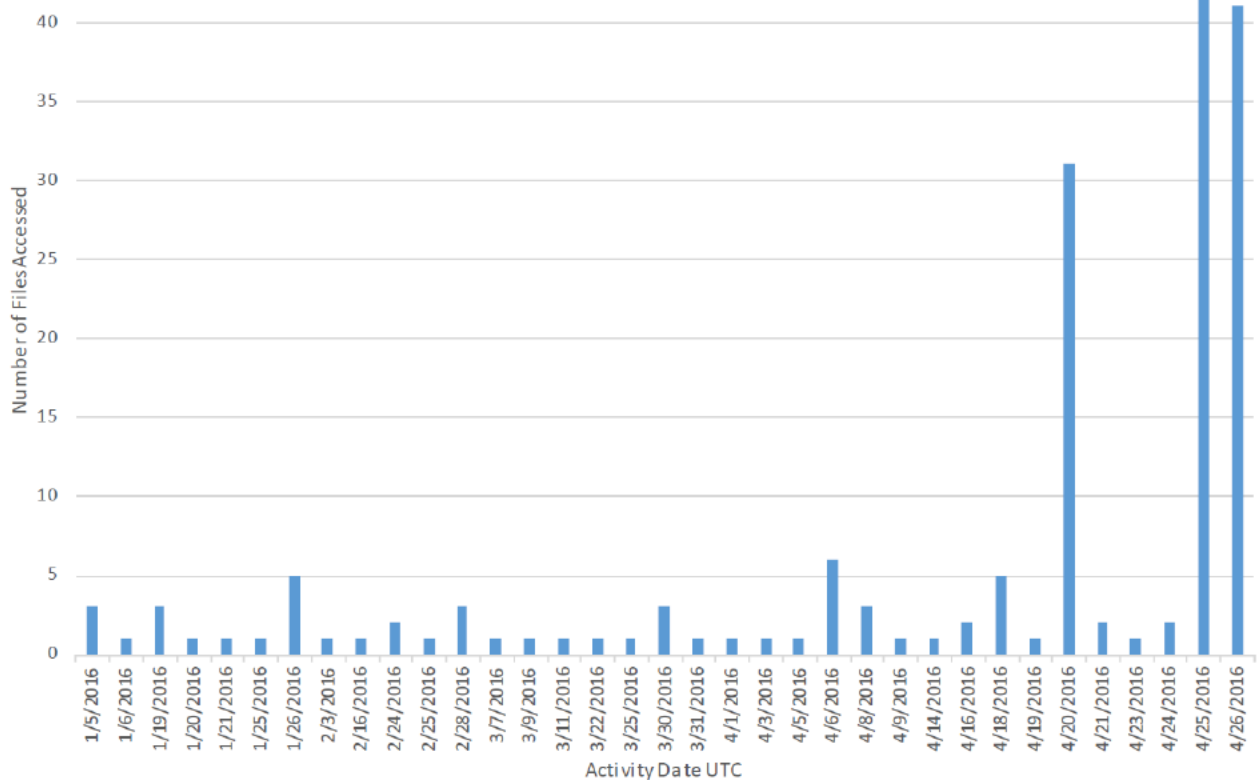
NAI-1504214559

BANDEMER DECL. ISO MICRON'S SUPPL.  
 OPP'N UMC'S TO MOTION TO DISMISS  
 Case No. 4:17-CV-06932-MMC

Ref # from Exhibit 4	Activity Date <sup>1</sup>	File Location	Server Location	File Name
	4/25/16 17:01	Laptop		
File 33	4/25/16 17:06	collab.micron.com	Boise USA	
	4/25/16 17:06	Laptop		
File 34	4/25/16 17:12	collab.micron.com	Boise USA	
	4/25/16 17:13	Laptop		

22. Chart 2 below illustrates the acceleration of access to United States based SharePoint servers detected on Wang's laptop prior to Mr. Wang's last day at Micron. This activity also coincides with an increase in file deletions and computer cleansing described above.

**Chart 2– Frequency chart illustrating Wang's accelerated access of United States Based SharePoint servers in late April, 2016**



1 **Access to R&D CAD Data in Boise Linux Server:**

2 23. In addition to the SharePoint downloading activity described above, the evidence  
3 from the Wang Laptop shows steps to obtain access to Micron's United States based proprietary  
4 Research and Development CAD ("R&D CAD") system hosted in Boise, Idaho. I understand  
5 that Micron system administrators in Boise informed Mr. Wang that, to access the R&D CAD  
6 system, he needed supervisor approval. Once that approval was obtained, the system  
7 administrators informed Mr. Wang that his "New Boise Linux account" had been activated.  
8 **(Clark Declaration Exhibits 6, 7 and 8** (attached to the Clark Declaration filed concurrently  
9 herewith) comprise the relevant emails between Mr. Wang and the system administrators of the  
10 Boise R&D server network).

11 24. Once Mr. Wang's Boise Linux account was activated, the R&D CAD system  
12 could be accessed using software called [REDACTED] which acts as a virtual desktop and  
13 allows the user to view the largely pictorial, schematic and graphical files contained in the R&D  
14 CAD system. Although no forensic artifacts are created that document which specific files are  
15 accessed, it is possible to detect when the [REDACTED] is activated and, therefore, when the R&D  
16 CAD system is accessed. Specifically, each time [REDACTED] connects to a server, a session log  
17 is created within the user's profile. I reviewed the [REDACTED] session evidence on the Wang  
18 Laptop and determined that the R&D CAD system was accessed on 28 separate days in 2016,  
19 including for 3 hours on April 26 – the day Mr. Wang left Micron.

20 25. In February 2016, shortly after Mr. Wang's request to set up a new Boise Linux  
21 account for the R&D CAD system, an enhanced screen-capture software program – "Greenshot  
22 Portable" – that by design leaves a small evidence footprint, was used on the Wang Laptop.  
23 Greenshot Portable is the type of program that would allow Mr. Wang to capture images of  
24 designs available on the R&D CAD system. While it is not possible to determine each and every  
25 time the Greenshot Portable was executed, evidence that Greenshot Portable was used on the  
26 Wang Laptop was captured from areas within the Windows registry, which is inaccessible to the  
27 user and stores historical executions of software called the "Userassist" and "Shimcache".  
28

26. The Wang Laptop also evidences activities consistent with the storage of R&D CAD images on the Wang Google Drive Account. Specifically, the Internet browser's cache file that was left in the Shadow Copy of the Wang Laptop hard drive evidences that, on February 29, 2016, a folder called "25nm 4G3D CAD data" was created on Google Drive. The evidence on the Wang Laptop shows only a partial list of files and folders created and maintained on Google Drive; it does not reveal the full contents of the Google Drive files and folders.

**Additional File Download and Transfer Evidence on Wang Laptop:**

27. In addition to the Sharepoint downloads and R&D CAD system access evidence on the Wang Laptop described above, in 2016, evidence on the Wang Laptop shows that there were several instances where large numbers of Micron files were mass downloaded/copied to the Wang Laptop as well as Micron files transferred to either an external storage device connected to the Wang Laptop or to the Wang Google Drive Account.

**Mass Micron File Downloads to Wang Laptop:**

28. Evidence on the Wang Laptop indicates that on several occasions in April 2016 large numbers of files were downloaded/copied to the Wang Laptop. In total, 260 files were downloaded/copied to the Wang Laptop in April 2016 with 64 of those files being downloaded/copied on April 25, 2016 one day before Wang's last day of employment. Of the 260 files downloaded/copied to the Wang Laptop in April 2016, 56 of those were determined to have come from Micron servers based in the United States. In all of 2016, this evidence reflects that a total of 287 files were download/copied to the Wang Laptop and were determined to have come from Micron servers based in the United States as enumerated in **Exhibit 5**. A true and correct copy of a spreadsheet, which contains a record of downloads to the Wang Laptop and is attached hereto as **Exhibit 5**.

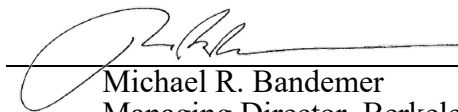
**Transfers to External Storage Device and the Wang Google Drive Account:**

29. Evidence on Wang's laptop also shows that over a thousand Micron files were transferred to external storage devices or to the Wang Google Drive Account. Micron's logs and forensic artifacts on Wang's laptop indicate that at least 1,274 unique Micron files and 38 folders were transferred to external storage devices or the Wang Google Drive Account in

1 2016. 108 of these Micron files were matched exclusively to files on Micron United States  
2 based servers. (See a true and correct copy of a spreadsheet created by my team, which contains  
3 those files transferred to a USB or Google Drive and is attached hereto as **Exhibit 6**). The  
4 complete contents of the folders described here cannot be determined without forensic analysis  
5 of the external storage devices that were used or the Wang Google Drive Account, which have  
6 not been made available to Micron at this time. In addition, as explained above, the evidence of  
7 the Wang Google Drive Account is only a partial view of the total files stored in this location.  
8 We know from the evidence that over 21 gigabytes was stored in the Wang Google Drive  
9 Account.

10 I declare under the penalty of perjury under the laws of the United States that the  
11 foregoing is true and correct.

12 Executed this 13 day of August 2018, in San Diego, California.

13  
14 

15 Michael R. Bandemer  
16 Managing Director, Berkeley Research Group, LLC  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28